PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-307580
(43)Date of publication of application : 28.11.1997

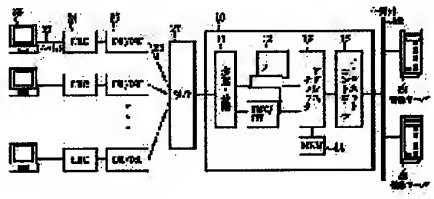
(51)Int.Cl. H04L 12/46
H04L 12/28
H04L 12/66

(21)Application number : 08-116345
(22)Date of filing : 10.05.1996

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : IRIE KAZUNARI
NISHIO GENICHI
OTA NORIHISA
MORIZAKI MASATO

(54) ILLEGAL PACKET PREVENTION METHOD AND BRIDGE

(57)Abstract:
PROBLEM TO BE SOLVED: To realize a stable computer communication network by comparing a combinations of addresses processed in protocols of different layers with a registered combination so as to abort a packet with a different address.
SOLUTION: The bridge 10 uses a multiplexer/demultiplexer circuit 11 to demultiplex a multiplexed signal into a channel signal of each subscriber and an HDLC processing circuit 12 detects a start and an end flag from an HDLC packet of each channel to decode an Ethernet packet. The decoded Ethernet packet is fed to an address check circuit 13. The circuit 13 compares a set of the Ethernet address and an IP address with a content of a memory table registered in advance in a memory 14 and aborts it to be an illegal packet when combination of packets differs from the registered content. Other packets than illegal packets are fed to an Ethernet controller 15, from which the packets are sent to a center side Ethernet 22 and sent to a subscriber side Ethernet 21 other than the transmitter source.



LEGAL STATUS

[Date of request for examination] 23.01.2001
[Date of sending the examiner's decision of rejection] 17.06.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] Correspondence of the address processed with the protocol of a mutually different layer by the bridge equipment which relays the packet-ized data between networks is registered beforehand. The first address which is included in the header of the packet transmitted and shows transmitting-in network of the packet origin, or the destination, The second address which is included in the data of the packet transmitted and shows the transmitting origin in the protocol of a high order layer or the destination is detected. The inaccurate packet prevention approach characterized by discarding the packet when the combination of the first address and the second address which were detected differs from all of the combination registered beforehand.
[Claim 2] Correspondence of the address processed with the protocol of a mutually different layer by the bridge equipment which relays the packet-ized data between networks is registered beforehand. When the data of the packet transmitted are the response to an inquiry of the address of the second layer using the address of the first layer, The inaccurate packet prevention approach characterized by discarding the packet when the combination of the address of the first layer and the address of the second layer which are included in the data of the packet differs from all of the combination registered beforehand.
[Claim 3] In the bridge equipment which relays the packet-ized data between networks A storage means by which the combination of the address processed with the protocol of a mutually different layer is registered beforehand, The first detection means which detects the first address which is included in the header of the packet transmitted and shows the transmitting origin of the packet, or the destination, The second detection means which detects the second address which is included in the data of the packet transmitted and shows the transmitting origin in the protocol of a high order layer, or the destination, Bridge equipment characterized by having a means to discard the packet when the combination of the first address detected by said first means and the second address detected by said second means differs from all of the combination registered into said storage means.
[Claim 4] In the bridge equipment which relays the packet-ized data between networks A storage means by which the combination of the address processed with the protocol of a mutually different layer is registered beforehand, A means to detect that the data of the packet transmitted are the response to an inquiry of the address of the second layer using the address of the first layer, With this first means Bridge equipment characterized by having a means to discard the packet when the combination of the address of the first layer and the address of the second layer which are included in the data of the detected packet differs from all of the

combination registered into said storage means.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the online communications which packet-ize data and transmit them. It is related with the bridge equipment which performs packet junction between networks especially. It is related with detection and prevention of an inaccurate packet with bridge equipment in more detail.
[0002] In this specification, what was connected by the "network" possible [transmission and reception of one or more terminals of a packet] is said. That is, the case where the number of terminals is "1" is included about some [at least] networks from which a packet is relayed by bridge equipment.
[0003]
[Description of the Prior Art] In the online communications which packet-ize data and transmit them between computers, in order to perform packet junction between networks, the bridge equipment which performs a packet transfer with the protocol of the data link layer of an OSI reference model is widely used from the former. Moreover, such bridge equipment is used also in order to hold two or more terminals. Below, the junction between the Ethernet through a subscriber line is explained to an example.
[0004] Drawing 8 is the block block diagram showing the bridge equipment 30 and its use gestalt of the conventional example. Bridge equipment 30 performs packet junction between two or more subscriber side Ethernet 21 and center side Ethernet 22. One or more subscriber terminals 23 and the low-end card (LEC) 24 are connected to subscriber side Ethernet 21, respectively, and the low-end card 24 is connected to a subscriber line 26 through the subscriber side terminating set 25, respectively. Termination of these subscriber lines 26 is carried out by the subscriber communication system terminating set 27 by the side of a network contractor (SLT:Subscriber Line Terminal), and they are connected to center side Ethernet 22 through bridge equipment 30. The information server 28 is shown in drawing as equipment (computer) connected to center side Ethernet 22.
[0005] As a subscriber terminal 23, a personal computer is used, for example. The low-end card 24 is a kind of bridge equipment, and performs the interface/protocol conversion between Ethernet and a subscriber line. When the communication line offered by the subscriber line 26 is an ISDN circuit or a digital dedicated line as a subscriber side terminating set 25, in the case of DSU (Digital Service Unit) and an optical-communication system, what is called ONU (Optical Network Unit) equipped with the photoelectricity signal transformation function is used. Metal or an optical fiber is used as a subscriber line 26, and a line connection is carried out by 64 kbit/s, 128 kbit/s, or 1.5 Mbit/s. Moreover, when the communication line offered by the subscriber line 26 is an analog network, a modem is used instead of the subscriber side terminating set 25.

[0006] Bridge equipment 30 is equipped with multiplex and the separation circuit 31, the HDLC processing circuit 32, and the Ethernet controller 33. Since two or more subscriber's-loop signals are multiplexed by the I/O signal of the subscriber communication system terminating set 27, to an input signal, it carries out multiplex [of multiplex and the separation circuit 31] to separation and a sending signal about the circuit for every subscriber. The HDLC processing circuit 32 extracts an Ethernet packet from the HDLC packet from a subscriber to a center side, and encapsulates the ISATTO packet from a center side to a subscriber to an HDLC packet. The Ethernet controller 33 performs the distribution by the side of the subscriber of an ether packet, or a center, and an interface function with center side Ethernet 22.
[0007] When performing a communication link from the subscriber terminal 23, the packet from the Ethernet interface with which the subscriber terminal 23 is equipped is first sent to the low-end card 24. The low-end card 24 processes the Ethernet packet which received with an HDLC (High-Level Data Link Control) protocol, encapsulates or maps it to HDLC packet data, and is transmitted to a network side by the communication line on a subscriber line 26. Before and after an Ethernet packet, an HDLC beginning flag and an ending flag are added and, specifically, it transmits. In addition, it is also possible to use the protocol of PPP (Point-to-Point Protocol) and others instead of HDLC.
[0008] Termination is carried out by the subscriber communication system terminating set 27, the signal of a multiple-line is multiplexed, and the HDLC packet sent out to the communication line on a subscriber line 26 is inputted into bridge equipment 30. With bridge equipment 30, multiplex and the separation circuit 31 separate the multiplexed signal into each subscriber's line signal, and an Ethernet packet is restored by next detecting initiation and an ending flag from the HDLC packet of each circuit in the HDLC processing circuit 32. The restored Ethernet packet is sent from bridge equipment 30 by the reverse procedure also to subscriber side Ethernet 21 different from a transmitting agency via the subscriber communication system terminating set 27, a subscriber line 26, the subscriber side terminating set 25, and the low-end card 24 while it is sent out to center side Ethernet 22 via the Ethernet controller 33.
[0009] Since useless traffic is reduced, if the destination of an Ethernet packet is in a center side like the information server 28, the packet will be transmitted only to center side Ethernet 22, and if the destination is in other subscribers side, the packet is turned up by the Ethernet controller 33, and it can also transmit to the subscriber terminal 23 of the destination. In this case, since the information which terminal is connected to which subscriber's loop (communication link port) or center side Ethernet is required, the Ethernet address of an Ethernet packet is learned and it holds on a memory table (not shown).
[0010]
[Problem(s) to be Solved by the Invention] With conventional bridge equipment, two or more communication link ports were usually prepared, it is detecting the Ethernet address of the terminal (computer) connected to the point of between all communication link ports or each communication link port, i.e., the 48-bit MAC (Media Access Control) address, and the packet transmission and reception between them were enabled. However, with conventional bridge equipment, although the Ethernet address could be learned, it was not able to check to the justification [address / which are processed by the high order layer / the IP address of the packet for IP communication link and the Ethernet address] of correspondence. For this reason, in order to become and clear up to other terminals a setting mistake and intentionally, for example, even when the same IP address as other terminals was set as a terminal, the packet from that terminal was passed as it is, and there was a problem that derangement arose in a communication link. Furthermore, it was also difficult to specify the terminal which has caused the problem in such a case.
[0011] This invention solves such a technical problem and aims at offering the inaccurate packet prevention approach and bridge equipment which can perform the online communications which prevented derangement of the communication link by the inaccurate packet by intentionally [of the address of a high order layer / a setting mistake or intentionally], and were stabilized.
[0012]
[Means for Solving the Problem] Correspondence of the address processed with the protocol of

a mutually different layer by the bridge equipment which the first viewpoint of this invention is the inaccurate packet prevention approach, and relays the packet-ized data between networks is registered beforehand. The first address which is included in the header of the packet transmitted and shows transmitting-in network of the packet origin, or the destination, The second address which is included in the data of the packet transmitted and shows the transmitting origin in the protocol of a high order layer or the destination is detected. When the combination of the first address and the second address which were detected differs from all of the combination registered beforehand, it is characterized by discarding the packet.

[0013] In performing IP (Internet Protocol) communication link by the high order layer, using Ethernet as a network, it compares with the group of the address registered beforehand about the group of the Ethernet address and the IP address which were given to the header and data of an Ethernet packet. And the packet is discarded when there is no match. Thereby, derangement of the communication link by the inaccurate packet by intentionally [of an IP address / a setting mistake or intentionally] can be prevented.

[0014] In the communication link between computers, even if the address of a high order layer is known, when the address of a lower layer is strange, multiple address transmission of the address of the high order layer is carried out, and getting to know the address of a lower layer by the response is performed. If it is the case of IP communication link, by carrying out multiple address transmission of the phase hand IP address by the ARP (Address Resolution Protocol) demand packet, and a phase hand's terminal answering it, and returning one's Ethernet address by the ARP response packet, it is a transmitting agency and a phase hand's Ethernet address can be known. Also in this case, the combination of the inaccurate address may be returned by intentionally [of a phase hand IP address / a setting mistake or intentionally].

[0015] The second viewpoint of this invention prevents such injustice, and correspondence of the address processed with the protocol of a mutually different layer by the bridge equipment which relays the packet-ized data between networks is registered beforehand. When the data of the packet transmitted are the response to an inquiry of the address of the second layer using the address of the first layer, When the combination of the address of the first layer and the address of the second layer which are included in the data of the packet differs from all of the combination registered beforehand, it is characterized by discarding the packet.

[0016] The ARP response packet encapsulated by the data of an Ethernet packet is specifically detected, and it compares with the group of the address beforehand registered about the group of the IP address of "the destination currently looked for" in the header of the ARP packet, and the Ethernet address. And the packet is discarded when there is no match.

[0017] In the bridge equipment which the third viewpoint of this invention is equipment which performs the approach of the first viewpoint, and relays the packet-ized data between networks A storage means by which the combination of the address processed with the protocol of a mutually different layer is registered beforehand, The first detection means which detects the first address which is included in the header of the packet transmitted and shows the transmitting origin of the packet, or the destination, The second detection means which detects the second address which is included in the data of the packet transmitted and shows the transmitting origin in the protocol of a high order layer, or the destination, When the combination of the first address detected by the first means and the second address detected by the second means differs from all of the combination registered into the storage means, it is characterized by having a means to discard the packet.

[0018] In the bridge equipment which the fourth viewpoint of this invention is equipment which performs the approach of the second viewpoint, and relays the packet-ized data between networks A storage means by which the combination of the address processed with the protocol of a mutually different layer is registered beforehand, A means to detect that the data of the packet transmitted are the response to an inquiry of the address of the second layer using the address of the first layer, When the combination of the address of the first layer and the address of the second layer which are included in the data of the packet detected by this first means differs from all of the combination registered into the storage means, it is characterized by having a means to discard that packet.

[0019]
[Embodiment of the Invention] Drawing 1 is the block block diagram showing the operation gestalt of this invention, and shows bridge equipment 10 and its use gestalt. Here, the junction between the Ethernet through a subscriber line is explained to an example.
[0020] In this operation gestalt, bridge equipment 10 performs packet junction between two or more subscriber side Ethernet 21 and center side Ethernet 22. One or more subscriber terminals 23 and the low-end card (LEC) 24 are connected to subscriber side Ethernet 21, respectively, and the low-end card 24 is connected to a subscriber line 26 through the subscriber side terminating set (ONU/DSU) 25, respectively. Termination of these subscriber lines 26 is carried out by the subscriber communication system terminating set (SLT) 27 by the side of a network contractor, and they are connected to center side Ethernet 22 through bridge equipment 10. The information server 28 and the management server 29 are shown in drawing as equipment (computer) connected to center side Ethernet 22.
[0021] Bridge equipment 10 is equipped with multiplex and the separation circuit 11, the HDLC processing circuit 12, the address checking circuit 13, memory 14, and the Ethernet controller 15. Since two or more subscriber's-loop signals are multiplexed by the I/O signal of the subscriber communication system terminating set 27, to an input signal, it carries out multiplex [of multiplex and the separation circuit 11] to separation and a sending signal about the circuit for every subscriber. The HDLC processing circuit 12 extracts an Ethernet packet from the HDLC packet from a subscriber to a center side, and encapsulates the ISATTO packet from a center side to a subscriber to an HDLC packet. The address checking circuit 13 checks the address information of an Ethernet packet, and discards the packet which has different address information from the contents beforehand registered into memory 14. The Ethernet controller 15 performs the distribution by the side of the subscriber of an ether packet, or a center, and an interface function with center side Ethernet 22.
[0022] Here, with reference to drawing 2 thru/or drawing 5 , a address resolution protocol (ARP) required for the communication link between the structure of an Ethernet packet and an IP packet and a terminal is explained.
[0023] Drawing 2 shows the structure of an Ethernet packet. The field which shows the classification (ETYPE) of the destination Ethernet address, the transmitting agency Ethernet address, and a higher-level protocol as a header is established in an Ethernet packet, and the frame-check-sequence field (FCS) for a data field and an error correction is further established in it.
[0024] Drawing 3 shows the rough structure of an IP packet, and drawing 4 shows detailed structure per 4 bytes. An IP packet is constituted by the header field and the data field, and these are stored in the data area of an Ethernet packet, and it is transmitted and received. Each field of a version, header length, a service type, IP packet size, a packet identifier, a flag, the offset for data division, a packet life time, the identifier for the upper layers, the checksum for headers, a transmitting agency IP address, a phase hand IP address, and an option is consisted of by the header field of an IP packet.
[0025] Drawing 5 shows the header structure of an ARP packet per 4 bytes. An ARP packet is also stored in the data area of an Ethernet packet, and is transmitted and received. The header of an ARP packet consists of each field of a hardware type, a protocol type, the die length of a hardware address, the die length of a protocol address, operation, the transmitting agency Ethernet address, a transmitting agency IP address, the destination Ethernet address currently looked for, and the destination IP address currently looked for. In order to communicate through Ethernet, the Ethernet address of a mutual terminal is required. For this reason, in IP communication link, it is necessary to obtain the Ethernet address of the terminal which has a phase hand IP address first. Then, broadcasting transmission of the ARP demand packet is carried out first. The terminal which has the IP address which corresponds to this ARP demand packet returns its Ethernet address as an ARP response packet. Thereby, the corresponding Ethernet address can be obtained. A communication link becomes possible by specifying a phase hand IP address and the Ethernet address by the predetermined address field henceforth. The distinction with an ARP demand and a response is recognized according to the contents of

assignment of an operation field.
[0026] With reference to drawing 1 , the actuation is explained again. When transmitting a packet from the subscriber terminal 23, the packet from the Ethernet interface with which the subscriber terminal 23 is equipped is first sent to the low-end card 24. The low-end card 24 processes the Ethernet packet which received with an HDLC protocol, encapsulates or maps it to HDLC packet data, and is transmitted to a network side by the communication line on a subscriber line 26. Before and after an Ethernet packet, an HDLC beginning flag and an ending flag are added and, specifically, it transmits. It is also possible to use the protocol of PPP and others instead of HDLC. Termination is carried out by the subscriber communication system terminating set 27, the signal of a multiple-line is multiplexed, and the HDLC packet sent out to the communication line on a subscriber line 26 is inputted into bridge equipment 10. With bridge equipment 10, multiplex and the separation circuit 11 separate the multiplexed signal into each subscriber's line signal, and an Ethernet packet is restored by next detecting initiation and an ending flag from the HDLC packet of each circuit in the HDLC processing circuit 12. Restoration processing of an Ethernet packet is performed to juxtaposition. The restored Ethernet packet is sent to the address checking circuit 13. If the address checking circuit 13 is the packet of a different combination from the contents of registration as compared with the contents of the memory table beforehand registered into memory 14, it will discard the group of the Ethernet address and an IP address as an inaccurate packet. Like [the Ethernet controller 15] delivery and the conventional example, a reverse procedure sends out packets other than an inaccurate packet also to subscriber side Ethernet 21 with an another transmitting agency while sending them out to center side Ethernet 22.
[0027] Drawing 6 shows the flow of the address checking circuit 13 of operation. Only in the case of the Ethernet packet containing the usual IP packet, as a candidate for a check of the address by the address checking circuit 13, the case of only the Ethernet packet containing an ARP packet and the case of the both sides can be considered. Here, the case where both sides are made applicable to a check is explained.
[0028] If an Ethernet packet is inputted, as for the address checking circuit 13, the contents of the data field will judge an IP packet or an ARP response packet. In the case of an IP packet, the transmitting origin included in the header of an Ethernet packet or the Ethernet address of the destination, and the IP address of the transmitting origin included in the header of an IP packet or the destination are detected, and the combination of the Ethernet address and the IP address which were detected, and the combination beforehand registered into the table in memory 14 are compared with it, and in differing from all, it discards the packet. Moreover, the combination of the Ethernet address of the destination and the IP address which are searching in the header of the ARP response packet when the contents of the data field of an Ethernet packet are ARP response packets is compared with the combination beforehand registered into the table in memory 14, and in differing from all, it discards the packet.
[0029] Considering the purpose which prevents an inaccurate packet, fundamentally, the check of an ARP packet is enough. However, an inaccurate packet can be more certainly prevented with checking the Ethernet packet containing the usual IP packet.
[0030] Drawing 7 shows an example of the table beforehand registered into memory 14. Correspondence with the Ethernet address for a subscription terminal and an IP address is registered into this table. The address checking circuit 13 and the correspondence relation of these addresses are checked. For example, in "the Ethernet address 1", a destination IP address discards [the destination Ethernet address] a packet by which the destination IP address is set as "IP address 2" in "the Ethernet address 1", although the destination Ethernet address passes the thing of "IP address 1." The same is said of an ARP packet, and although it is made to pass when the Ethernet address is set as "the Ethernet address 1" for the IP address of the destination which is searching in the header of an ARP response packet by "IP address 1", the packet in which one of the addresses differs from the contents of the table discards.
[0031] As an approach of registering such a table into memory 14, although creating with bridge equipment 10 is also possible, it is convenient to create and transmit by the general purpose computer or workstation on a network. That is, a table is created by the management server 29

and it transmits to bridge equipment 10 by the approach of of FTP (File Transfer Protocol), or SNMP (Simple Network Managentnt Protocol) and others. According to this approach, it is controllable at RIMOTO.

[0032] Since useless traffic is reduced like the conventional example also in this operation gestalt, if the destination of an Ethernet packet is in a center side like the information server 28, that packet will be transmitted only to center side Ethernet 22, and if the destination is in other subscribers side, that packet is turned up by the Ethernet controller 15, and it can also transmit to the subscriber terminal 23 of the destination. In this case, the information which terminal is connected to which subscriber's loop (communication link port) or center side Ethernet is required. Then, the Ethernet address of an Ethernet packet is learned with bridge equipment 10, and it holds on the memory table. This memory table is shared with the table for an inaccurate packet check, and the amount of memory can be reduced by using the table of a gestalt to which port information was added.

[0033] With the operation gestalt explained above, it confirms whether to be what is beforehand registered in the group of an IP address and the Ethernet address, and since a different inaccurate Ethernet packet from registration information discards, it can prevent derangement of the communication link by the inaccurate packet.

[0034] Although the operation gestalt explained above explained the case where a communication line and center side Ethernet were connected to the example, the configuration which connects two or more Ethernet to the port of direct bridge equipment can carry out this invention similarly. Moreover, it is also possible to consider as the configuration which connects the terminal for control to bridge equipment, and changes a memory table directly, without using a management server. Furthermore, although the gestalt which checks IP communication link about the combination of the Ethernet address and an IP address for an example was explained, an inaccurate packet can be similarly prevented by carrying out an address check similarly to higher-level protocols other than IP.

[0035]

[Effect of the Invention] As explained above, it confirms whether the inaccurate packet prevention approach and bridge equipment of this invention are in agreement with what was registered beforehand about correspondence of the address processed with the protocol of a mutually different layer in online communications, and a different packet from what was registered discards. There is effectiveness it is ineffective to it being possible for this to realize the computer communication network which derangement of the communication link by the inaccurate packet did not arise, and was stabilized.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block block diagram showing the operation gestalt of this invention.

[Drawing 2] Drawing showing the structure of an Ethernet packet.

[Drawing 3] Drawing showing the rough structure of an IP packet.
[Drawing 4] Drawing showing the detailed structure of an IP packet.
[Drawing 5] Drawing showing the header structure of an ARP packet.
[Drawing 6] Drawing showing the flow of an address checking circuit of operation.
[Drawing 7] Drawing showing an example of the table beforehand registered into memory.
[Drawing 8] The block block diagram showing the bridge equipment and its use gestalt of the conventional example.
[Description of Notations]
10 30 Bridge equipment
11 31 Multiplex and separation circuit
12 32 HDLC processing circuit
13 Address Checking Circuit
14 Memory
15 33 Ethernet controller
21 Subscriber Side Ethernet
22 Center Side Ethernet
23 Subscriber Terminal
24 Low-end Card
25 Subscriber Side Terminating Set
26 Subscriber Line
27 Subscriber Communication System Terminating Set
28 Information Server
29 Management Server

[Translation done.]

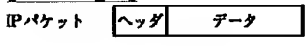
* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

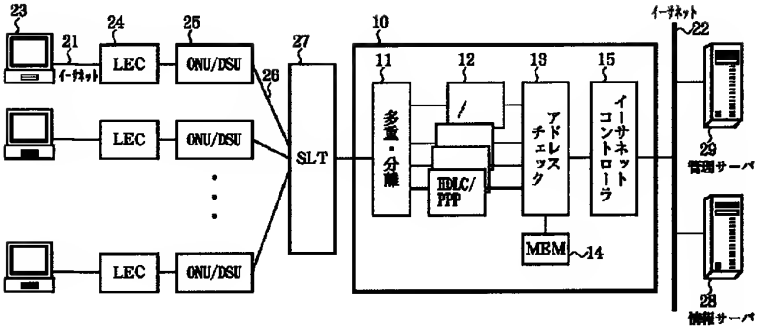
DRAWINGS

[Drawing 3]



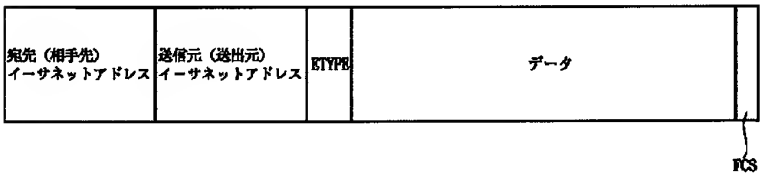
IPパケットの構造

[Drawing 1]



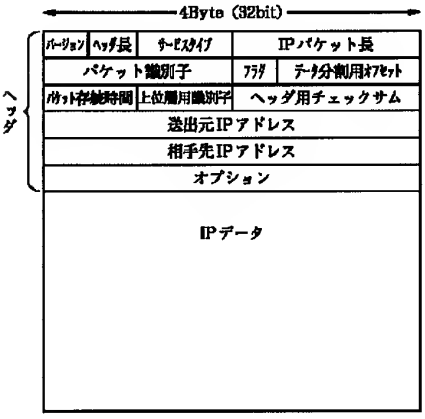
[Drawing 2]

イーサネットパケットの構造



[Drawing 4]

< IPv4 >



IPパケットの内訳構成

[Drawing 5]

ARPパケットの構造

4Byte

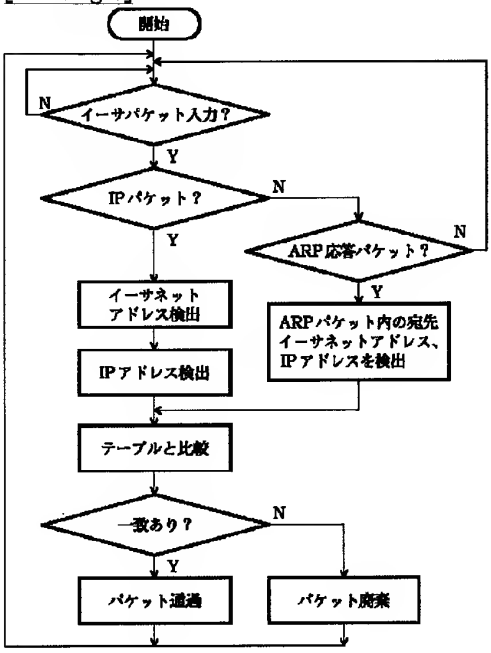
ハードウェアタイプ	プロトコルタイプ
HLEN / PLEN	オペレーション
送出元イーサネットアドレス	
送出元イーサネットアドレス（続き）	送出元IPアドレス
送出元IPアドレス（続き）	探している宛先イーサネットアドレス
探している宛先イーサネットアドレス（続き）	
探している宛先IPアドレス	

HLEN ：ハードウェアアドレスの長さ
PLEN ：プロトコルアドレスの長さ

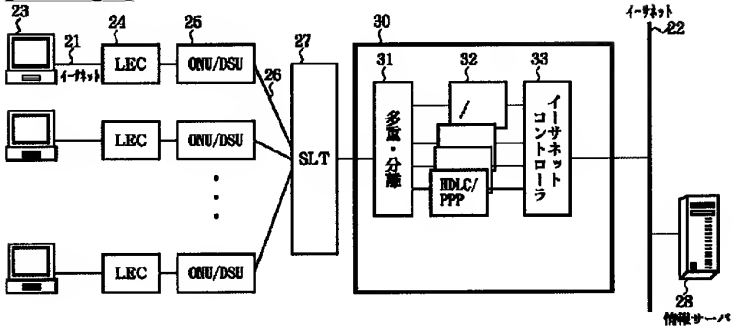
[Drawing 7]

イーサネットアドレス1	IPアドレス1
イーサネットアドレス2	IPアドレス2
イーサネットアドレス3	IPアドレス3
⋮	⋮

[Drawing 6]



[Drawing 8]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平9－307580

(43)公開日　平成９年(1997)11月28日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/46			Ｈ０４Ｌ	11/00	３１０Ｃ
	12/28		9466－5K		11/20	Ｂ
	12/66					

審査請求　未請求　請求項の数４　ＯＬ　（全 ８ 頁）

(21)出願番号　特願平8－116345

(22)出願日　平成８年(1996) ５月10日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　入江　一成
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　西尾　弦一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　太田　紀久
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　井出　直孝　（外１名）

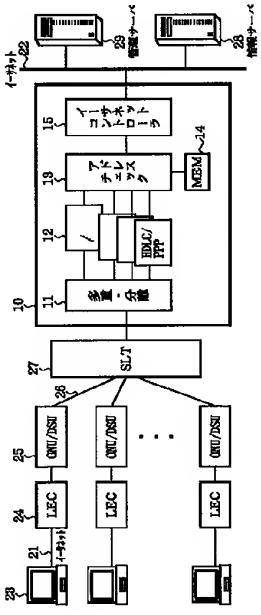
最終頁に続く

(54)【発明の名称】　不正パケット防止方法およびブリッジ装置

(57)【要約】

【課題】　コンピュータ間でデータをパケット化して伝送する場合に、パケット内のデータに含まれる上位レイヤのプロトコルで使用されるアドレスの不正を防止する。

【解決手段】　二つのレイヤのプロトコルで使用するアドレスの組み合わせをあらかじめ登録しておき、受信したパケットからその二つのレイヤのそれぞれのアドレスを検出してあらかじめ登録された組み合わせと比較し、一致するものがない場合にはそのパケットを廃棄する。



1

【特許請求の範囲】

【請求項１】　パケット化されたデータをネットワーク間で中継するブリッジ装置に互いに異なるレイヤのプロトコルで処理されるアドレスの対応をあらかじめ登録しておき、

転送されるパケットのヘッダに含まれそのパケットのネットワーク内での送信元または宛先を示す第一のアドレスと、転送されるパケットのデータに含まれ上位レイヤのプロトコルにおける送信元または宛先を示す第二のアドレスとを検出し、

検出された第一のアドレスと第二のアドレスとの組み合わせがあらかじめ登録された組み合わせのいずれとも異なる場合にはそのパケットを廃棄することを特徴とする不正パケット防止方法。

【請求項２】　パケット化されたデータをネットワーク間で中継するブリッジ装置に互いに異なるレイヤのプロトコルで処理されるアドレスの対応をあらかじめ登録しておき、

転送されるパケットのデータが第一のレイヤのアドレスを用いた第二のレイヤのアドレスの問い合わせに対する応答であるとき、そのパケットのデータに含まれる第一のレイヤのアドレスと第二のレイヤのアドレスとの組み合わせがあらかじめ登録された組み合わせのいずれとも異なる場合にはそのパケットを廃棄することを特徴とする不正パケット防止方法。

【請求項３】　パケット化されたデータをネットワーク間で中継するブリッジ装置において、

互いに異なるレイヤのプロトコルで処理されるアドレスの組み合わせがあらかじめ登録される記憶手段と、

転送されるパケットのヘッダに含まれそのパケットの送信元または宛先を示す第一のアドレスを検出する第一の検出手段と、

転送されるパケットのデータに含まれ上位レイヤのプロトコルにおける送信元または宛先を示す第二のアドレスを検出する第二の検出手段と、

前記第一の手段により検出された第一のアドレスと前記第二の手段により検出された第二のアドレスとの組み合わせが前記記憶手段に登録された組み合わせのいずれとも異なる場合にはそのパケットを廃棄する手段とを備えたことを特徴とするブリッジ装置。

【請求項４】　パケット化されたデータをネットワーク間で中継するブリッジ装置において、

互いに異なるレイヤのプロトコルで処理されるアドレスの組み合わせがあらかじめ登録される記憶手段と、

転送されるパケットのデータが第一のレイヤのアドレスを用いた第二のレイヤのアドレスの問い合わせに対する応答であることを検出する手段と、

この第一の手段により検出されたパケットのデータに含まれる第一のレイヤのアドレスと第二のレイヤのアドレスとの組み合わせが前記記憶手段に登録された組み合わせのいずれとも異なる場合にはそのパケットを廃棄する手段とを備えたことを特徴とするブリッジ装置。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデータをパケット化して伝送するコンピュータ通信に関する。特に、ネットワーク間のパケット中継を行うブリッジ装置に関する。さらに詳しくは、ブリッジ装置での不正パケットの検出および防止に関する。

【０００２】本明細書において「ネットワーク」とは、１以上の端末がパケットの送受信可能に接続されたものをいう。すなわち、ブリッジ装置によりパケットが中継される少なくとも一部のネットワークについて、その端末数が「１」の場合を含む。

【０００３】

【従来の技術】コンピュータ間でデータをパケット化して伝送するコンピュータ通信においては、ネットワーク間のパケット中継を行うため、ＯＳＩ参照モデルのデータリンク層のプロトコルでパケット転送を行うブリッジ装置が従来から広く用いられている。また、このようなブリッジ装置は、複数の端末を収容するためにも用いられる。以下では、加入者線を介したイーサネット間の中継を例に説明する。

【０００４】図８は従来例のブリッジ装置３０およびその利用形態を示すブロック構成図である。ブリッジ装置３０は複数の加入者側イーサネット２１とセンタ側イーサネット２２との間のパケット中継を行う。加入者側イーサネット２１にはそれぞれ１以上の加入者端末２３とローエンドカード（ＬＥＣ）２４とが接続され、ローエンドカード２４はそれぞれ加入者側終端装置２５を介して加入者線２６に接続される。これらの加入者線２６はネットワーク業者側の加入者通信系終端装置（ＳＬＴ：Subscriber Line Terminal）２７により終端され、ブリッジ装置３０を介してセンタ側イーサネット２２に接続される。図には、センタ側イーサネット２２に接続された装置（コンピュータ）として、情報サーバ２８を示す。

【０００５】加入者端末２３としては、例えばパーソナルコンピュータが用いられる。ローエンドカード２４は一種のブリッジ装置であり、イーサネットと加入者線との間のインタフェース／プロトコル変換を行う。加入者側終端装置２５としては、加入者線２６により提供される通信回線がＩＳＤＮ回線あるいはディジタル専用回線の場合にはＤＳＵ（Digital Service Unit）、光通信系の場合には光電気信号変換機能を備えたＯＮＵ（Optical Network Unit）と呼ばれるものが用いられる。加入者線２６としてはメタルあるいは光ファイバが用いられ、６４ｋｂｉｔ／ｓ、１２８ｋｂｉｔ／ｓあるいは１．５Ｍｂｉｔ／ｓで回線接続する。また、加入者線２６により提供される通信回線がアナログ回線の場合には、加入

者側終端装置２５の代わりにモデムが用いられる。

【０００６】ブリッジ装置３０は、多重・分離回路３１、ＨＤＬＣ処理回路３２およびイーサネットコントローラ３３を備える。多重・分離回路３１は、加入者通信系終端装置２７の入出力信号に複数の加入者回線信号が多重化されていることから、各加入者毎の回線について、受信信号に対しては分離、送信信号に対しては多重する。ＨＤＬＣ処理回路３２は、加入者からセンタ側へのＨＤＬＣパケットからイーサネットパケットを抽出し、センタ側から加入者へのイーサットパケットをＨＤＬＣパケットにカプセル化する。イーサネットコントローラ３３は、イーサパケットの加入者側あるいはセンタ側への振り分け、およびセンタ側イーサネット２２とのインタフェース機能を実行する。

【０００７】加入者端末２３から通信を行う場合、その加入者端末２３が備えているイーサネットインタフェースからのパケットは、最初にローエンドカード２４に送られる。ローエンドカード２４は、受信したイーサネットパケットをＨＤＬＣ（High-Level Data Link Control）プロトコルにより処理し、ＨＤＬＣパケットデータにカプセル化あるいはマッピングして、加入者線２６上の通信回線によりネットワーク側に送信する。具体的には、イーサネットパケットの前後にＨＤＬＣ開始フラグと終了フラグとを付加して送信する。なお、ＨＤＬＣの代わりにＰＰＰ（Point-to-Point Protocol ）その他のプロトコルを用いることも可能である。

【０００８】加入者線２６上の通信回線に送出されたＨＤＬＣパケットは加入者通信系終端装置２７により終端され、複数回線の信号が多重化されてブリッジ装置３０に入力される。ブリッジ装置３０では、その多重化された信号を多重・分離回路３１により各加入者の回線信号に分離し、次にＨＤＬＣ処理回路３２において各回線のＨＤＬＣパケットから開始および終了フラグを検出することによりイーサネットパケットを復元する。復元されたイーサネットパケットは、イーサネットコントローラ３３を経由してセンタ側イーサネット２２に送出されるとともに、送信元とは別の加入者側イーサネット２１に対しても、逆の手順により、ブリッジ装置３０から加入者通信系終端装置２７、加入者線２６、加入者側終端装置２５およびローエンドカード２４を経由して送られる。

【０００９】無駄なトラヒックを低減するため、イーサネットパケットの宛先が情報サーバ２８のようなセンタ側にあればそのパケットをセンタ側イーサネット２２のみに送信し、宛先が他の加入者側にあればイーサネットコントローラ３３でそのパケットを折り返して宛先の加入者端末２３に送信することもできる。この場合、どの端末がどの加入者回線（通信ポート）あるいはセンタ側イーサネットに接続されているかという情報が必要であるため、イーサネットパケットのイーサネットアドレスを学習し、メモリテーブル（図示せず）に保持する。

【００１０】

【発明が解決しようとする課題】従来のブリッジ装置では、通常は複数の通信ポートが設けられ、全通信ポートの間あるいは各通信ポートの先に接続されている端末（コンピュータ）のイーサネットアドレス、すなわち４８ビットのＭＡＣ（Media Access Control）アドレスを検知することで、それらの間のパケット送受信を可能としていた。しかし、従来のブリッジ装置では、イーサネットアドレスを学習することはできるが、上位レイヤで処理されるＩＰ通信用パケットのＩＰアドレスとイーサネットアドレスとの対応の正当性までチェックすることはできなかった。このため、例えば設定ミスや故意に他の端末になりすますために他の端末と同じＩＰアドレスが端末に設定された場合でも、その端末からのパケットをそのまま通過させ、通信に混乱が生じるという問題があった。さらに、そのような場合に、問題を起こしている端末を特定することも困難であった。

【００１１】本発明は、このような課題を解決し、上位レイヤのアドレスの設定ミスや故意による不正パケットによる通信の混乱を防止して安定したコンピュータ通信を行うことのできる不正パケット防止方法およびブリッジ装置を提供することを目的とする。

【００１２】

【課題を解決するための手段】本発明の第一の観点は不正パケット防止方法であり、パケット化されたデータをネットワーク間で中継するブリッジ装置に互いに異なるレイヤのプロトコルで処理されるアドレスの対応をあらかじめ登録しておき、転送されるパケットのヘッダに含まれそのパケットのネットワーク内での送信元または宛先を示す第一のアドレスと、転送されるパケットのデータに含まれ上位レイヤのプロトコルにおける送信元または宛先を示す第二のアドレスとを検出し、検出された第一のアドレスと第二のアドレスとの組み合わせがあらかじめ登録された組み合わせのいずれとも異なる場合にはそのパケットを廃棄することを特徴とする。

【００１３】ネットワークとしてイーサネットを用い、上位レイヤでＩＰ（Internet Protocol ）通信を行う場合には、イーサネットパケットのヘッダおよびデータに付与されたイーサネットアドレスとＩＰアドレスとの組について、あらかじめ登録されたアドレスの組と比較する。そして、一致するものがない場合には、そのパケットを廃棄する。これにより、ＩＰアドレスの設定ミスや故意による不正パケットによる通信の混乱を防止できる。

【００１４】コンピュータ間の通信では、上位レイヤのアドレスが既知であっても下位レイヤのアドレスが未知の場合、その上位レイヤのアドレスを同報送信し、その応答により下位レイヤのアドレスを知ることが行われている。ＩＰ通信の場合であれば、ＡＲＰ（Address Reso

lution Protocol ）要求パケットにより相手先ＩＰアドレスを同報送信し、相手先の端末がそれに応答してＡＲＰ応答パケットにより自分のイーサネットアドレスを返送することで、送信元で相手先のイーサネットアドレスを知ることができる。このような場合にも、相手先ＩＰアドレスの設定ミスや故意により、不正なアドレスの組み合わせが返送される可能性がある。

【００１５】本発明の第二の観点はこのような不正を防止するものであり、パケット化されたデータをネットワーク間で中継するブリッジ装置に互いに異なるレイヤのプロトコルで処理されるアドレスの対応をあらかじめ登録しておき、転送されるパケットのデータが第一のレイヤのアドレスを用いた第二のレイヤのアドレスの問い合わせに対する応答であるとき、そのパケットのデータに含まれる第一のレイヤのアドレスと第二のレイヤのアドレスとの組み合わせがあらかじめ登録された組み合わせのいずれとも異なる場合にはそのパケットを廃棄することを特徴とする。

【００１６】具体的には、イーサネットパケットのデータにカプセル化されたＡＲＰ応答パケットを検出し、そのＡＲＰパケットのヘッダ内の「探している宛先」のＩＰアドレスとイーサネットアドレスとの組について、あらかじめ登録されたアドレスの組と比較する。そして、一致するものがない場合には、そのパケットを廃棄する。

【００１７】本発明の第三の観点は第一の観点の方法を実行する装置であり、パケット化されたデータをネットワーク間で中継するブリッジ装置において、互いに異なるレイヤのプロトコルで処理されるアドレスの組み合わせがあらかじめ登録される記憶手段と、転送されるパケットのヘッダに含まれそのパケットの送信元または宛先を示す第一のアドレスを検出する第一の検出手段と、転送されるパケットのデータに含まれ上位レイヤのプロトコルにおける送信元または宛先を示す第二のアドレスを検出する第二の検出手段と、第一の手段により検出された第一のアドレスと第二の手段により検出された第二のアドレスとの組み合わせが記憶手段に登録された組み合わせのいずれとも異なる場合にはそのパケットを廃棄する手段とを備えたことを特徴とする。

【００１８】本発明の第四の観点は第二の観点の方法を実行する装置であり、パケット化されたデータをネットワーク間で中継するブリッジ装置において、互いに異なるレイヤのプロトコルで処理されるアドレスの組み合わせがあらかじめ登録される記憶手段と、転送されるパケットのデータが第一のレイヤのアドレスを用いた第二のレイヤのアドレスの問い合わせに対する応答であることを検出する手段と、この第一の手段により検出されたパケットのデータに含まれる第一のレイヤのアドレスと第二のレイヤのアドレスとの組み合わせが記憶手段に登録された組み合わせのいずれとも異なる場合にはそのパケットを廃棄する手段とを備えたことを特徴とする。

【００１９】

【発明の実施の形態】図１は本発明の実施形態を示すブロック構成図であり、ブリッジ装置１０とその利用形態を示す。ここでは、加入者線を介したイーサネット間の中継を例に説明する。

【００２０】この実施形態において、ブリッジ装置１０は複数の加入者側イーサネット２１とセンタ側イーサネット２２との間のパケット中継を行う。加入者側イーサネット２１にはそれぞれ１以上の加入者端末２３とローエンドカード（ＬＥＣ）２４とが接続され、ローエンドカード２４はそれぞれ加入者側終端装置（ＯＮＵ／ＤＳＵ）２５を介して加入者線２６に接続される。これらの加入者線２６はネットワーク業者側の加入者通信系終端装置（ＳＬＴ）２７により終端され、ブリッジ装置１０を介してセンタ側イーサネット２２に接続される。図には、センタ側イーサネット２２に接続された装置（コンピュータ）として、情報サーバ２８および管理サーバ２９を示す。

【００２１】ブリッジ装置１０は、多重・分離回路１１、ＨＤＬＣ処理回路１２、アドレスチェック回路１３、メモリ１４およびイーサネットコントローラ１５を備える。多重・分離回路１１は、加入者通信系終端装置２７の入出力信号に複数の加入者回線信号が多重化されていることから、各加入者毎の回線について、受信信号に対しては分離、送信信号に対しては多重する。ＨＤＬＣ処理回路１２は、加入者からセンタ側へのＨＤＬＣパケットからイーサネットパケットを抽出し、センタ側から加入者へのイーサットパケットをＨＤＬＣパケットにカプセル化する。アドレスチェック回路１３は、イーサネットパケットのアドレス情報をチェックし、あらかじめメモリ１４に登録されている内容と異なるアドレス情報を有するパケットを廃棄する。イーサネットコントローラ１５は、イーサパケットの加入者側あるいはセンタ側への振り分け、およびセンタ側イーサネット２２とのインタフェース機能を実行する。

【００２２】ここで、図２ないし図５を参照して、イーサネットパケット、ＩＰパケットの構造ならびに端末間の通信に必要なアドレス解決プロトコル（ＡＲＰ）について説明する。

【００２３】図２はイーサネットパケットの構造を示す。イーサネットパケットには、ヘッダとして宛先イーサネットアドレス、送信元イーサネットアドレスおよび上位プロトコルの種別（ＥＴＹＰＥ）を示すフィールドが設けられ、さらに、データフィールドおよび誤り訂正のためのフレームチェックシーケンスフィールド（ＦＣＳ）が設けられる。

【００２４】図３はＩＰパケットの概略的な構造を示し、図４は詳しい構造を４バイト単位に示す。ＩＰパケットはヘッダフィールドとデータフィールドとにより構

成され、これらがイーサネットパケットのデータ領域に収められて送受信される。ＩＰパケットのヘッダフィールドには、バージョン、ヘッダ長、サービスタイプ、ＩＰパケット長、パケット識別子、フラグ、データ分割用オフセット、パケット存続時間、上位層用識別子、ヘッダ用チェックサム、送信元ＩＰアドレス、相手先ＩＰアドレス、およびオプションの各フィールドから構成される。

【００２５】図５はＡＲＰパケットのヘッダ構造を４バイト単位に示す。ＡＲＰパケットもまた、イーサネットパケットのデータ領域に収められて送受信される。ＡＲＰパケットのヘッダは、ハードウェアタイプ、プロトコルタイプ、ハードウェアアドレスの長さ、プロトコルアドレスの長さ、オペレーション、送信元イーサネットアドレス、送信元ＩＰアドレス、探している宛先イーサネットアドレス、探している宛先ＩＰアドレスの各フィールドから構成される。イーサネットを介して通信を行うためには、互いの端末のイーサネットアドレスが必要である。このためＩＰ通信においては、始めに相手先ＩＰアドレスを有する端末のイーサネットアドレスを得る必要がある。そこで、最初にＡＲＰ要求パケットをブロードキャスト送信する。このＡＲＰ要求パケットに対して該当するＩＰアドレスを有する端末は、自分のイーサネットアドレスをＡＲＰ応答パケットとして返送する。これにより、該当するイーサネットアドレスを得ることができる。以降は、相手先ＩＰアドレスとイーサネットアドレスとを所定のアドレスフィールドで指定することにより、通信が可能となる。ＡＲＰ要求と応答との区別は、オペレーションフィールドの指定内容により認識する。

【００２６】再び図１を参照してその動作を説明する。加入者端末２３からパケットを送信する場合、その加入者端末２３が備えているイーサネットインタフェースからのパケットは、最初にローエンドカード２４に送られる。ローエンドカード２４は、受信したイーサネットパケットをＨＤＬＣプロトコルにより処理し、ＨＤＬＣパケットデータにカプセル化あるいはマッピングして、加入者線２６上の通信回線によりネットワーク側に送信する。具体的には、イーサネットパケットの前後にＨＤＬＣ開始フラグと終了フラグとを付加して送信する。ＨＤＬＣの代わりにＰＰＰその他のプロトコルを用いることも可能である。加入者線２６上の通信回線に送出されたＨＤＬＣパケットは加入者通信系終端装置２７により終端され、複数回線の信号が多重化されてブリッジ装置１０に入力される。ブリッジ装置１０では、その多重化された信号を多重・分離回路１１により各加入者の回線信号に分離し、次にＨＤＬＣ処理回路１２において各回線のＨＤＬＣパケットから開始および終了フラグを検出することによりイーサネットパケットを復元する。イーサネットパケットの復元処理は並列に行われる。復元されたイーサネットパケットはアドレスチェック回路１３に送られる。アドレスチェック回路１３は、イーサネットアドレスとＩＰアドレスとの組をメモリ１４にあらかじめ登録されたメモリテーブルの内容と比較し、登録内容と異なる組み合わせのパケットであれば不正パケットとして廃棄する。不正パケット以外のパケットはイーサネットコントローラ１５に送り、従来例と同様に、センタ側イーサネット２２に送出するとともに、送信元とは別の加入者側イーサネット２１に対しても逆の手順により送出する。

【００２７】図６はアドレスチェック回路１３の動作フローを示す。アドレスチェック回路１３によるアドレスのチェック対象としては、通常のＩＰパケットを含むイーサネットパケットのみの場合、ＡＲＰパケットを含むイーサネットパケットのみの場合、およびその双方の場合が考えられる。ここでは、双方をチェック対象とする場合について説明する。

【００２８】イーサネットパケットが入力されると、アドレスチェック回路１３は、そのデータフィールドの内容がＩＰパケットかＡＲＰ応答パケットかを判断する。ＩＰパケットの場合には、イーサネットパケットのヘッダに含まれる送信元または宛先のイーサネットアドレスと、ＩＰパケットのヘッダに含まれる送信元または宛先のＩＰアドレスとを検出し、検出されたイーサネットアドレスとＩＰアドレスとの組み合わせとメモリ１４内のテーブルにあらかじめ登録された組み合わせとを比較し、いずれとも異なる場合にはそのパケットを廃棄する。また、イーサネットパケットのデータフィールドの内容がＡＲＰ応答パケットの場合には、そのＡＲＰ応答パケットのヘッダ内の探している宛先のイーサネットアドレスとＩＰアドレスとの組み合わせと、メモリ１４内のテーブルにあらかじめ登録された組み合わせとを比較し、いずれとも異なる場合にはそのパケットを廃棄する。

【００２９】不正パケットを防止する目的からすると、基本的には、ＡＲＰパケットのチェックで十分である。ただし、通常のＩＰパケットを含むイーサネットパケットをもチェックすることで、不正パケットをより確実に防止することができる。

【００３０】図７はメモリ１４にあらかじめ登録されるテーブルの一例を示す。このテーブルには、加入端末分のイーサネットアドレスとＩＰアドレスとの対応が登録される。アドレスチェック回路１３と、これらのアドレスの対応関係をチェックする。例えば、宛先イーサネットアドレスが「イーサネットアドレス１」で宛先ＩＰアドレスが「ＩＰアドレス１」のものは通過させるが、宛先イーサネットアドレスが「イーサネットアドレス１」で宛先ＩＰアドレスが「ＩＰアドレス２」に設定されているようなパケットは廃棄する。ＡＲＰパケットについても同様で、ＡＲＰ応答パケットのヘッダ内の探してい

る宛先のＩＰアドレスが「ＩＰアドレス１」でイーサネットアドレスが「イーサネットアドレス１」に設定されている場合は通過させるが、いずれかのアドレスがテーブルの内容と異なるパケットは廃棄する。

【００３１】このようなテーブルをメモリ１４内に登録する方法としては、ブリッジ装置１０で作成することも可能であるが、ネットワーク上の汎用コンピュータあるいはワークステーションで作成して転送することが便利である。すなわち、管理サーバ２９によりテーブルを作成し、ＦＴＰ（File Transfer Protocol）あるいはＳＮＭＰ（Simple Network Managentnt Protocol）その他の方法によりブリッジ装置１０に転送する。この方法によれば、リモートで制御可能である。

【００３２】この実施形態においても従来例と同様に、無駄なトラヒックを低減するため、イーサネットパケットの宛先が情報サーバ２８のようなセンタ側にあればそのパケットをセンタ側イーサネット２２のみに送信し、宛先が他の加入者側にあればイーサネットコントローラ１５でそのパケットを折り返して宛先の加入者端末２３に送信することもできる。この場合、どの端末がどの加入者回線（通信ポート）あるいはセンタ側イーサネットに接続されているかという情報が必要である。そこで、ブリッジ装置１０でイーサネットパケットのイーサネットアドレスを学習し、メモリテーブルに保持しておく。このメモリテーブルを不正パケットチェック用のテーブルと共用し、ポート情報を追加した形態のテーブルを使用することで、メモリ量を低減できる。

【００３３】以上説明した実施形態では、ＩＰアドレスとイーサネットアドレスとの組をあらかじめ登録されているものかどうかチェックし、登録情報と異なる不正イーサネットパケットは廃棄するため、不正パケットによる通信の混乱を防止することができる。

【００３４】以上説明した実施形態では、通信回線とセンタ側イーサネットとを接続する場合を例に説明したが、複数のイーサネットを直接ブリッジ装置のポートに接続する構成でも同様に本発明を実施できる。また、管理サーバを用いずに、制御用端末をブリッジ装置に接続して直接にメモリテーブルを変更する構成とすることも可能である。さらに、ＩＰ通信を例にイーサネットアドレスとＩＰアドレスとの組み合わせについてチェックす＊る形態について説明したが、ＩＰ以外の上位プロトコルに対しても同様にアドレスチェックすることにより、同様に不正パケットを防止することができる。

【００３５】

【発明の効果】以上説明したように、本発明の不正パケット防止方法およびブリッジ装置は、コンピュータ通信における互いに異なるレイヤのプロトコルで処理されるアドレスの対応について、あらかじめ登録されたものと一致するかどうかをチェックし、登録されたものと異なるパケットは廃棄する。これにより、不正パケットによる通信の混乱が生じることがなく、安定したコンピュータ通信ネットワークを実現することが可能となる効果がある。

【図面の簡単な説明】

【図１】本発明の実施形態を示すブロック構成図。

【図２】イーサネットパケットの構造を示す図。

【図３】ＩＰパケットの概略的な構造を示す図。

【図４】ＩＰパケットの詳しい構造を示す図。

【図５】ＡＲＰパケットのヘッダ構造を示す図。

【図６】アドレスチェック回路の動作フローを示す図。

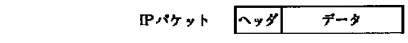
【図７】メモリにあらかじめ登録されるテーブルの一例を示す図。

【図８】従来例のブリッジ装置およびその利用形態を示すブロック構成図。

【符号の説明】

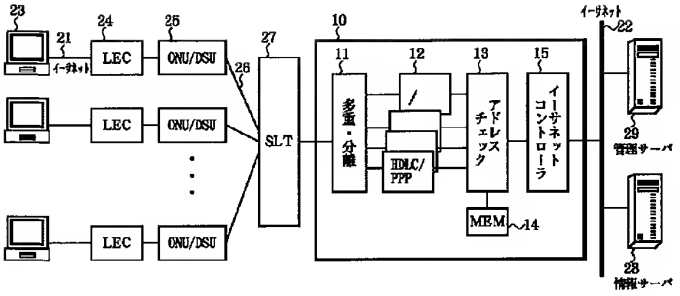
１０、３０　ブリッジ装置
１１、３１　多重・分離回路
１２、３２　ＨＤＬＣ処理回路
１３　アドレスチェック回路
１４　メモリ
１５、３３　イーサネットコントローラ
２１　加入者側イーサネット
２２　センタ側イーサネット
２３　加入者端末
２４　ローエンドカード
２５　加入者側終端装置
２６　加入者線
２７　加入者通信系終端装置
２８　情報サーバ
２９　管理サーバ

【図３】



IPパケットの構造

【図1】

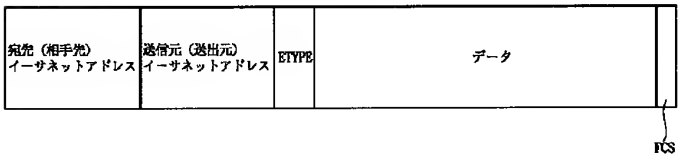


【図7】

イーサネットアドレス1	IPアドレス1
イーサネットアドレス2	IPアドレス2
イーサネットアドレス3	IPアドレス3
⋮	⋮

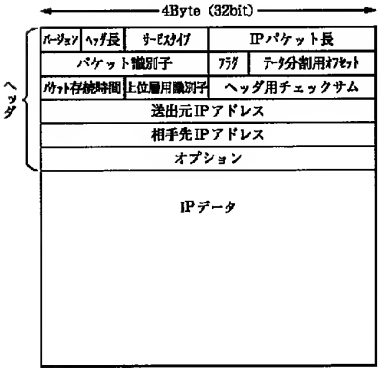
【図2】

イーサネットパケットの構造



【図4】

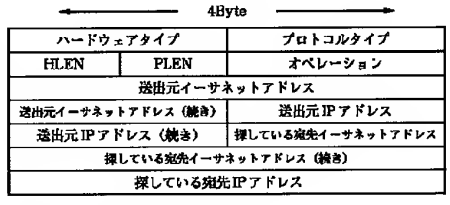
<IPv4>



IPパケットの内訳構成

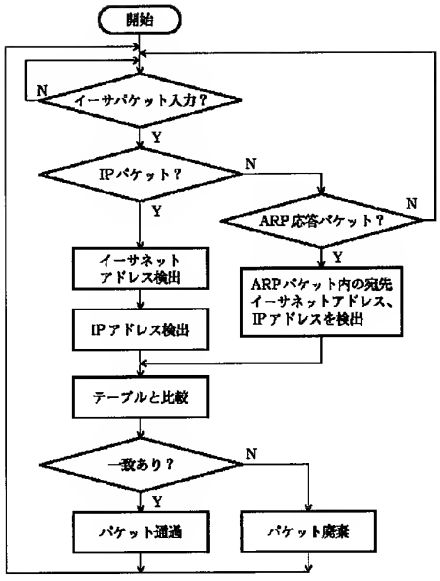
【図5】

ARPパケットの構造

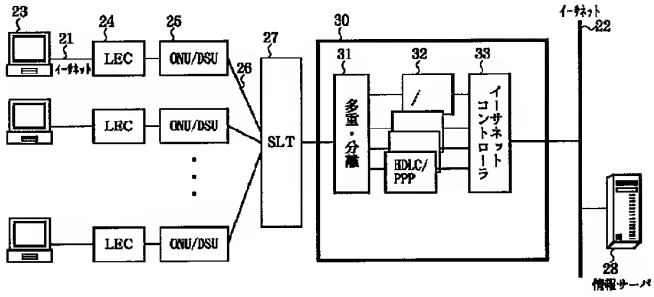


HLEN ：ハードウェアアドレスの長さ
PLEN ：プロトコルアドレスの長さ

【図６】



【図８】



フロントページの続き

(72)発明者　森崎　正人
東京都新宿区西新宿三丁目19番２号　日本
電信電話株式会社内